ON CYBER PATROL ™

As covered or mandated by AR 25-2

Phish On!

It's that time of year again! The long winter chill is lifting, flowers are blooming, April is nearing, and the fish …I mean "Phish" are biting. That's right, and by "Phish," I mean "you" soldier. The tax season is here once again, and the cyber predators are well rested from a long winter's break, hoping to add you as a feather in their cap.

The IRS is warning taxpayers to beware of unsolicited emails that appear to be from either the IRS or an organization closely linked to the IRS, such as the Electronic Federal Tax Payment System (EFTPS). Suspicious emails attempting to get your personal information should be ignored. Bear in mind that the IRS would never request personal or financial info via email, nor would it request information from you by text message or social media sites.

Remember, valid professional organizations will never request private information or credentials via email. So be wary of emails asking for your log-in information, Social Security Number (SSN), or Tax Identification Number (TIN). Never click on links in emails promising large sums of money, or urgently requesting you to log-in to verify your information. In order to help the Army identify and mitigate these problems, do your part and quickly report suspicious e-mails. If you are on a military installation and receive a suspicious e-mail, report it to your local Information Assurance Manger (IAM), or Network Enterprise Center (NEC) immediately. If you are not on a military installation, report it to your local RCERT immediately.

Twenty years ago was the "birth" of email as we know it. While the internet and the use of email systems have opened many doors and provided vast opportunities, we must always remain vigilant to ensure certain doorways remain secure. It is the responsibility of every soldier and civilian to practice precaution and best judgment when accessing the internet with any type of device.

So, keep yourself safe and make sure that when cyber criminals go phishing, you're the "one that got away".